AMENDMENTS

In the claims:

The following shows the status of all pending claims:

C1

1. (Currently Amended) An electronic tender system for accepting as a contract price the highest or lowest price among bids, comprising:

a bidder sub-system including:

a predefined set of code parameters in which a different code parameter is associated with each of respective bid amounts within a tenderable range,

a code parameter acquisition section for acquiring a ~~predetermined~~ code parameter from said predefined set of code parameters corresponding to a bid amount selected by the bidder sub-system within a tenderable range,

a code processing section for encoding the bid selected by the bidder sub-system using the ~~predetermined~~ acquired code parameter obtained by said code parameter acquisition section, and

a transmission section for sending a message including an encoded bid encoded by said coding section to a tender opening sub-system, and

a tender opening sub-system including:

a reception section for receiving messages from bidder sub-systems including encoded bids until a closing time,

a predefined set of decode parameters in which a different decode parameter is associated with each of respective contract price candidates,

a candidate price selection section for sequentially selecting contract price candidates beginning with one of a highest and a lowest within said tenderable range,

a decode parameter acquisition section for acquiring from said predefined set of decode parameters a ~~predetermined~~ decode parameter corresponding to a contract price candidate selected by the selection section, and

a determination section for decoding encoded bids using ~~a predetermined~~ an acquired decode parameter corresponding to a contract price candidate selected by the selection section to determine whether a bid that is the same as the contract price candidate selected by the selection section exists among encoded bids received by the reception section.

2. (Currently Amended) The electronic tender system as claimed in claim 1, wherein the code processing section of the bidder sub-system encodes a bid value using the ~~predetermined~~ code parameter obtained by the code parameter acquisition section from the predefined set of code parameters, and

wherein the reception section of the tender opening sub-system includes a decoding section for sequentially decoding encoded bids received by the reception section using the ~~predetermined~~ decode parameter acquired by the decode parameter acquisition section from the predefined set of decode parameters, and a judgment section for judging that a coded bid is identical to a contact price candidate selected by the selection section when the decoding result is equal to a fixed value.

3. (Currently Amended) The electronic tender system as claimed in claim 1, wherein the ~~code processing section of the bidder sub-system performs encoding using a predetermined~~ predefined set of code parameters comprises respective public keys each corresponding to ~~the~~ a different bid amount, and

wherein the decoding section of the tender opening sub-system performs a decoding operation using a the predefined set of decode parameters comprises respective secret keys each corresponding to the ~~predetermined~~ a respective one of the public keys corresponding to ~~the contract price candidates~~said different bid amounts.

4. (Currently Amended) The electronic tender system as claimed in claim 2, wherein the ~~code processing section of the bidder sub-system performs encoding using a predetermined~~ predefined set of code parameters comprises respective public keys each corresponding to ~~the~~ a different bid amount, and

wherein the decoding section of the tender opening sub-system performs a decoding operation using a the predefined set of decode parameters comprises respective secret keys each corresponding to the ~~predetermined~~ a respective one of the public keys corresponding to ~~the contract price candidates~~said different bid amounts.

5. (Currently Amended) The electronic tender system as claimed in claim 1, wherein said tender opening sub-system includes an announcement section for announcing one of a portion of a ~~predetermined~~ decode parameter acquired by the decode parameter acquisition section and decoding results obtained in the determination section for each contract price candidate.

6. (Currently Amended) The electronic tender system as claimed in claim 2, wherein said tender opening sub-system includes an announcement section for announcing one of a portion of a ~~predetermined~~ decode parameter acquired by the decode parameter acquisition section and decoding results obtained in the determination section for each contract price candidate.

7. (Currently Amended) The electronic tender system as claimed in claim 3, wherein said tender opening sub-system includes an announcement section for announcing one of a portion of a ~~predetermined~~ decode parameter acquired by the decode parameter acquisition section and decoding results obtained in the determination section for each contract price candidate.

8. (Currently Amended) The electronic tender system as claimed in claim 4, wherein said tender opening sub-system includes an announcement section for announcing one of a portion of a ~~predetermined~~ decode parameter acquired

by the decode parameter acquisition section and decoding results obtained in the determination section for each contract price candidate.

9. (Currently Amended) A method for placing a bid for a contract, comprising:

~~determining~~ choosing a bid price to be used in a bid;

obtaining a ~~predetermined~~ code parameter ~~corresponding to~~associated with the chosen bid price from a predefined set of code parameters in which a different code parameter is associated with each of respective bid prices~~, wherein different predetermined code parameters correspond to respective different bid prices~~;

encoding the bid ~~in accordance with~~ using the ~~predetermined~~ code parameter associated with the chosen bid price in the predefined set; and

transmitting a message including the encoded bid to a bid receiving system.

10. (Currently Amended) A method for determining a contract price from received bids, comprising:

receiving a plurality of encoded bids for a contract;

~~determining~~ obtaining a ~~predetermined~~ decode parameter ~~corresponding to~~ that is associated with one of a highest and a lowest contract price candidate within a tenderable range of the contract from a predefined set of decode parameters in which a different decode parameter is associated with each of respective contract price candidates~~, wherein different predetermined decode parameters correspond to respective different contract price candidates~~;

attempting to decode each of ~~said plurality of~~ the encoded bids using ~~said predetermined~~ the obtained decode parameter;

if at least one of ~~said plurality of~~the encoded bids is decodeable using ~~said predetermined~~ the obtained decode parameter, determining that ~~said~~ the contract price is equal to a price of said at least one encoded bid; and

if none of ~~said plurality of~~the encoded bids is decodeable using ~~said predetermined~~ the obtained decode parameter, ~~determining~~ obtaining a next

~~predetermined~~ decode parameter ~~corresponding to~~ from the predefined set of decode parameters that is associated with a next closest contract price candidate with respect to the highest or lowest contract price candidate within the tenderable range of the contract, and attempting to decode each of ~~said plurality of~~ the encoded bids using ~~said~~ the next obtained ~~predetermined~~ decode parameter,

wherein said plurality of bids are attempted to be decoded using successive ~~predetermined~~ decode parameters corresponding to successive contract price candidates until at least one bid is successfully decoded.

11. (New) The method claimed in claim 9, wherein said predefined set of code parameters comprises respective public keys associated with each bid price in the set.

12. (New) The method claim in claim 11, wherein encoding a bid using the code parameter associated with the chosen bid price comprises encoding the bid using the public key associated with that bid price in the predefined set of code parameters.

13. (New) The method claimed in claim 10, wherein said predefined set of decode parameters comprises respective secret keys each associated with a corresponding public key used to encode bids of the associated contract price candidate.

14. (New) The method claim in claim 13, wherein attempting to decode each of the encoded bids using the obtained decode parameter comprises attempting to decode each of the encoded bids using the secret key associated with the contract price candidate.

REMARKS

The 1 May 2003 official action addressed claims 1-10. Claims 1-10 are amended. Claims 11-14 are added. Claims 1-14 are pending.

1. Overview of Amendments

Claim amendments

Independent claims 1 and 9 are amended to clarify that code parameters and are obtained from predefined sets of code parameters in which a different code parameters is associated with each of respective bid prices.

Independent claims 1 and 10 are amended to clarify that decode parameters and are obtained from predefined sets of decode parameters in which a different decode parameter is associated with each of respective contract price candidates.

Claims 2-8 are amended to be consistent with claim 1.

New claims 11-12 and 13-14 depend from claims 9 and 10, respectively, and specify that the recited code and decode parameters are public keys and secret keys, respectively.

No new matter is added.

2. Response to rejections

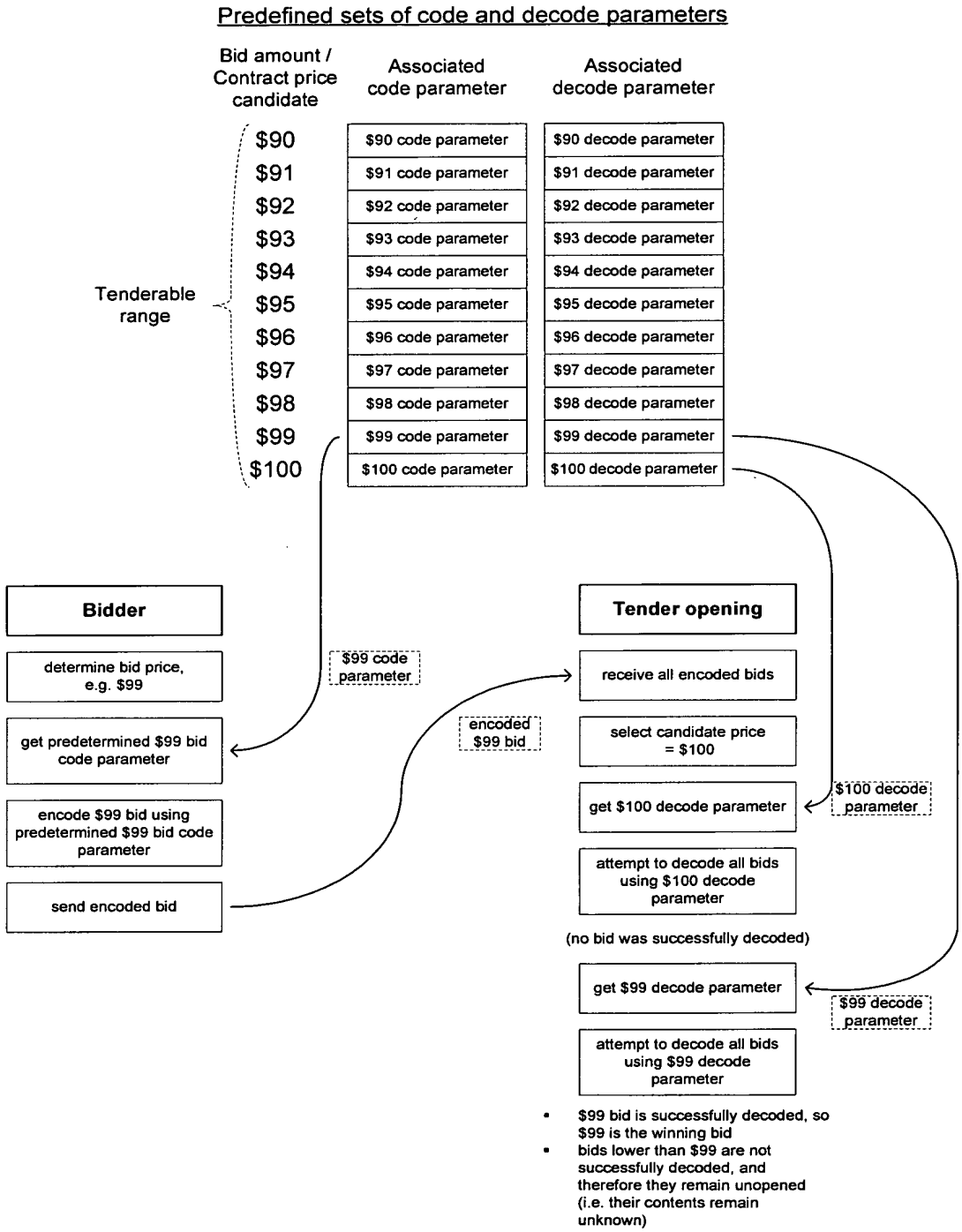
Prior art rejections

All claims are rejected as being anticipated by or obvious in view of Franklin (U.S. 6,055,518). Applicant has again reviewed Franklin in detail. Applicant respectfully maintains its position that Franklin is virtually unrelated to the features presently claimed. The examiner is respectfully requested to consider the points below. The undersigned will contact the examiner after filing this reply to arrange a telephone conference for the purpose of determining the reasons for any continuing disagreement.

Claimed invention

The claimed invention is directed to a system for auctions. A goal of the claimed invention is to determine the winning bid without revealing the contents of non-winning bids, thereby preserving the anonymity of the non-winning bidders and the amounts of their bids.

The features of the claimed system are illustrated in the following figure:



The claimed system codes and decodes bids using predefined sets of code and decode parameters (typically public keys and secret keys, respectively). Specifically, for each possible bid amount, there is a corresponding different code parameter (e.g. public key) that is used to code bids of that amount. Therefore, once a bidder chooses a bid amount, the bidder then obtains the code parameter (e.g. public key) that was previously defined as being the code parameter for bids of that amount, and the bid is coded using that code parameter. Therefore, for example, all bids of $99 will be encoded using the same public key that was previously defined as the $99 bid code parameter.

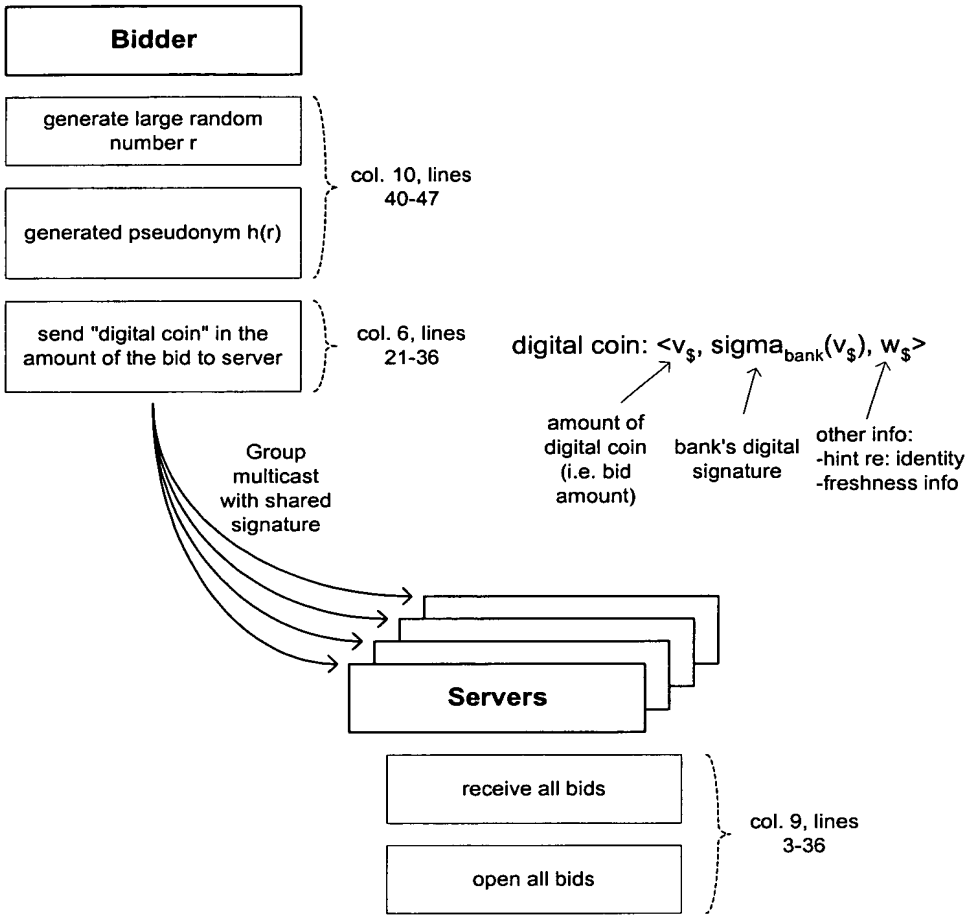
For each possible bid amount there is also a predefined decode parameter that corresponds to that bid amount and that works to decode data that has been coded using the code parameter associated with that bid amount. For example, the code parameter for $99 bids will have a corresponding decode parameter, which is also associated with $99 bids.

Consequently, to decode all bids without revealing the contents of non-winning bids, system attempts to decode all received bids using the decode parameter for the highest (or lowest) bid, and then the next decode parameter, and so on until a bid is successfully decoded.

Further description relating to the drawing above is provided in applicant's previous reply, which is incorporated herein by reference.

The Franklin reference

The Franklin system is significantly different than the system presently claimed. The following illustration shows Franklin's basic system:



Franklin submits bids in the form of a "digital coin," which is a form of electronic money that Franklin describes at col. 6, lines 21-36. The bidder may avoid disclosing his identity by using a pseudonym generated from a random number. A piece of each bid is transmitted to a different server through a group multicast process, as described at col. 4, line 18 - col. 5, line 64, and at col. 8, line 47 - col. 9, line 2. The piece of the bid that is transmitted to a particular server S_i is encoded using that server's public key K_i (col. 7, lines 10-20; col. 8, lines 36-40). The pieces of the bids are received by the respective servers, decrypted, and shared to reconstruct each bid, as described at col. 9, lines 3-21. Bids determined to be invalid through this process are discarded. All bids are then opened and consistency among the portions is inspected, as described at col. 9, lines 22-36. Bids determined to be invalid through this process are also discarded. The validity of the "digital coin" contained in each bid is then confirmed, as explained at col. 9, lines 7-53. While Franklin's system is

complex, it is sufficient for present purposes to recognize that Franklin validates bids using multicast, public and private keys, and digital coins, and that this process involves opening all bids.

Comparison of Franklin to present claims

Franklin does not have a predefined set of code parameters in which a different code parameter is associated with each bid, and Franklin does not use such a set of parameters to determine how to encode a bid. If Franklin had these features, then Franklin would describe a process in which the type of coding to be performed on the bid is determined by looking at the amount of the bid and then choosing a code parameter that has a predefined association with that amount. Franklin does not describe such a process. In Franklin, the bidder uses a server's public key to encrypt the part of the bid that is sent to that server, and the amount of the bid is not considered in determining the key used to encrypt the bid (col. 7, lines 10-20; col. 8, lines 36-40).

In the rejection of claim 9, the official action asserted that "obtaining a code parameter corresponding to the bid price" is taught at col. 10, lines 40-47, and that "the parameter would inherently be predetermined as the parameter corresponds to a particular bid." This assessment is believed to be incorrect. Col. 10, lines 40-47 state the following:

> A first requirement to achieving bidder anonymity is to remove the identity of the bidder at bidding terminals B_1, B_2, B_3 and B_n from the auction protocol of the preferred embodiment. A simple approach to achieve this is for each bidder, prior to submitting a bid, to generate a large random number r and use h(r) as a pseudonym for that bid, where h is a message digest function. That is, a bid would be submitted in a multicast as denoted by 500 in Fig. 5.

It is believed to be clear that this passage has nothing to do with a predefined set of code parameters in which a different code parameter corresponds to each bid price.

Therefore there is no support in Franklin for rejection of claims including these features, such as independent claims 1 and 9 and their dependent claims.

Franklin also does not have a predefined set of decode parameters in which a different decode parameter is associated with each contract price candidate, and Franklin does not apply decode parameters associated with successive contract price candidates until bids are decoded, making them the winning bids. If Franklin had these features, then Franklin would describe a process in which it is attempted to decode all bids by applying first one and then another decode parameter, selecting the decode parameters based on the contract price candidates that they are associated with in a predefined set. Franklin does not describe such a process. Franklin's bid opening process is clearly described under the heading "Opening The Bids" in col. 9. That process involves multiple servers performing a variety of tasks, one of which is implicitly the decoding of the encoded bids received by the server. But as noted above, the bids are encoded using public keys that are specific to individual servers, not to contract price candidates. Nothing in Franklin suggests that there is a predefined set of decode parameters corresponding to contract price candidates that is used in the bid opening process, and there is no reason to use such decode parameters since the bids were not encoded in a corresponding manner. Therefore there is no support in Franklin for rejection of claims including these features, such as independent claims 1 and 9 and their dependent claims.

In the rejections of claims 1 and 10, the official action asserts that selecting a decode parameter corresponding to a contract price candidate and applying decode parameters corresponding to successive contract price candidates is taught by Franklin at col. 10, line 52 - col. 11, line 15 and in Franklin claim 10. This assessment is believed to be incorrect. Col. 10, line 52 - col. 11, line 15 states the following:

> The auction would then proceed as before, except that the winner would be announced by S_i as follows:
>
> aid,h(r),σ_{Si}(aid,h(r))
>
> Note that S_i, not knowing the identity or location of the bidder that submit the bid with pseudonym h(r), must simply broadcast the declaration of the winner. Alternatively, S_i could place this signed declaration in a location

> from which it could be later retrieved by the winning bidder. The winner can employ t + 1 such declarations and the number r, which only it knows, as its ticket for claiming the auctioned item.
>
> While at first this may seem to ensure the bidder's anonymity, other steps may be required due to the properties of off-line digital cash. As discussed before, off-line cash schemes require that the customer's (in this case, the bidder's) identity be embedded within the value $v_\$$ in a way that reveals this identity to the bank if the same coin is spent multiple times. Thus, with proposed off-line cash schemes, if a bidder were to submit the same coin to two auctions (e.g., submit the coin to one, lose the auction, and submit the coin to another), then the identity of the bidder could be inferred by a coalition of one faulty auction server from each auction. Perhaps even worse, if $\sigma_{bank}(v_\$)$is ever leaked to the coalition of faulty servers (e.g., due to a weakness in the procedures by which the coin is reconstructed and deposited after it wins the second auction), then they could deposit both uses of the coin, thereby revealing the bidder's identity to the bank and "framing" the bidder for reusing the coin. It is possible to modify proposed off-line cash schemes so that the identity information embedded in $v_\$$ is encrypted with a key known only to the bank and the bidder. Then, the bank's cooperation would be required to reveal the identity of the bidder. However, this approach still enables the coalition of auction servers to link the same coin, and thus the same (unknown) bidder, to both auctions, and does not prevent the "framing" attack described above.

Again it is believed to be clear that this passage has nothing to do with the feature for which it is cited, namely a predefined set of decode parameters in which a different decode parameter corresponds to each contract price candidate, and the application of decode parameters corresponding to successive contract price candidates to attempt to decode one or more bids.

Therefore there is no support in Franklin for rejection of claims including these features, such as independent claims 1 and 10 and their dependent claims.

The foregoing amendments and remarks address all bases for rejection and are believed to place the case in condition for allowance. The undersigned will contact the examiner to set up a telephone conference to determine whether any issues remain that would prevent allowance.

Respectfully submitted,

Date: October 31, 2003

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

Ronald Coslick
Registration No. 36,489